Exec

Vulnerable to TOCTOU issues

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 9670 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Indeterminate File/Path • TOCTOU - Time of Check, Time of Use
Software Context	• Shell Functions
Location	• unistd.h
Description	The exec() class of functions are used for executing a file as a process image. The exec() family of calls are vulnerable to TOCTOU attacks. A call to a exec() family function should be flagged if the first argument (the directory or file name) is used earlier in a "check" category call.
APIs	

Function Name	Comments
_execl	use
_execle	use
_execlp	use
_execlpe	use
_execv	use
_execve	use
_execvp	use
_execvpe	use
_texecl	use
_texecle	use
_texeclp	use
_texeclpe	use

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

_texecv	use
_texecve	use
_texecvp	use
_texecvpe	use
_wexecl	use
_wexecle	use
_wexeclp	use
_wexeclpe	use
_wexecv	use
_wexecve	use
_wexecvpe	use
exec	use
execl	use
execle	use
execlp	use
execv	use
execve	use
execvp	use

Method of Attack

The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results.

The exec() call is a "use" category call that when preceded by a "check" category call can be indicative of a TOCTOU vulnerability.

A TOCTOU attack in regards to exec() can occur for example when

a. Check for existence of a file to be executed occurs.

b. exec() is called

Between a and b, an attacker can, for example, use a link to link the file to be executed to a different file and for which the subsequent exec() call will have clearly unexpected results.

This is an extremely serious vulnerability, since the attack profile is not constrained to profile of the "check" function.

Exception Criteria

Solutions

Solution Applicability	Solution Description	Solution Efficacy
Generally applicable.	The most basic advice for TOCTOU vulnerabilities is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help to limit the false sense of security given by the check.	Does not resolve the underlying vulnerability but limits the false sense of security given by the check.
Generally applicable.	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
Generally applicable.	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.

	Generally applicable. | Recheck the resource after the use call to verify that the action was taken appropriately. | Effective in some cases.
Signature Details	int execv (const char *filename, char *const argv[]) int execl (const char *filename, const char *arg0, ...) int execvp (const char *filename, char *const argv[]) int execlp (const char *filename, const char *arg0, ...)

Examples of Incorrect Code	`...`
	`if (stat("text.exe", &stat_p) != -1) {`
	`if ((status = execl("text.exe", 0)) == -1) {`
	`perror("Parent - Execl failed");`
	`exit(EXIT_FAILURE);`
	`}`
	`}`
	`...`

Examples of Corrected Code	`...`
	`if ((status = execl("text.exe", 0)) == -1) {`
	`perror("Execl failed");`
	`exit(EXIT_FAILURE);`
	`}`
	`...`

Source References	• Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, ch 9 • man page for exec() • Microsoft Developer Network Library (MSDN). • The GNU C Library. Executing a File[2]. • HP C Run-Time Library Reference Manual for OpenVMS Systems. OpenVMS Alpha Signal-Handling Notes[3] (2005).
Recommended Resource	
Discriminant Set	**Operating System**: • UNIX **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com